PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS AND INTERFERENCES

Application No.	:	10/560,345	Confirmation No.: 9362
Applicant	:	Vincent DeGroot	
Filed	:	June 7, 2006	
Title	:	METHOD FOR MONITORING A FIELD DEVICE	
TC/A.U.	:	2857	
Examiner	:	H. D. Wachsman	
Docket No.	:	DEGR3003 /FJD	
Customer No.	:	23364	

BRIEF ON APPEAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA. 22202-3514

Sir:

INTRODUCTORY COMMENTS

Pursuant to the provisions of 37 CFR 41.37, submitted herewith is Applicant/Appellant's Brief on Appeal along with the required fee.

Any additional fees necessary for this appeal may be charged to the undersigned's Deposit Account No. 02-0200.

REAL PARTY IN INTEREST

(37 CFR 41.37(c)(1)(i)

The real party in interest is Applicant/Appellant's assignee Endress + Hauser process Solutions AG. The assignment was recorded on June 29, 2006 at Reel 017874 and Frame 0264.

RELATED APPEALS AND INTERFERENCES

(37 CFR 41.37(c)(1)(ii)

There are no related appeals or interferences with respect to the invention defined in this application.

STATUS OF CLAIMS

(37 CFR 41.37(c)(1)(iii))

Claims 1 - 13 and 20 have been cancelled

Claims 14 - 19 and 21 - 28 are pending in this appeal.

Claims 14 - 19 and 21 - 28 have been finally rejected, which are the claims on appeal.

STATUS OF AMENDMENTS

(37 CFR 41.37(c)(1)(iv))

An amendment in the form of a REQUEST FOR RECONSIDERATION WITH AMENDMENT was filed after issuance of the Office Action of January 13, 2009, which presented a final rejection of claims 14 - 19 and 21 - 28. The amendment in the REQUEST FOR RECONSIDERATION WITH AMENDMENT was to the title portion of the drawing description and did not involve the claims.

Of the rejected claims, claims 14 and 26 are in independent form.

SUMMARY OF CLAIMED SUBJECT MATTER

(37 CFR 41.37 (c)(1)(v))

(References are to page and line of the specification)

The claimed subject matter relates to a method for monitoring a field device connected via a data bus with a control unit. In process automation technology, field devices are often used for the registering and/or influencing of process variables. Examples of such field devices are fill level measuring devices, mass flow measuring devices, pressure and temperature measuring devices, pH-redox potential measuring devices, conductivity measuring devices, etc., which, as sensors, register the corresponding process variables fill level, flow rate,

pressure, temperature, pH-value and conductivity (pg 1, lines 6 - 12).

Field devices in modern manufacturing plants are frequently connected with superordinated units, e.g. control systems or control units, via a field bus system. These superordinated units serve for process control, process visualization, process monitoring, as well as for operating and monitoring of field devices. From the superordinated units, communication connections to further company networks are also possible (pg. 2, lines 1 - 8).

The method according to independent claim 14 first defines a method step whereby the control unit is used at intervals in time to request an individual identifier of the field device (pg 4, lines 25 and 26). Following the request a comparison of the requested individual identifier is made with an identifier stored in the control unit in order to prevent unauthorized tampering with the field device (pg. 4, lines26 - 28). Then an alarm or some form of warning is produced in the case of a change in the requested individual identifier (pg. 5, lines 18 -19).

According to independent claim 26, the initial step is defined in terms of directing a query to the field device by the control unit at time intervals, which query is answered by the field device, and if there is no answer then this information is stored in a data base along with a corresponding time stamp (pg. 5, lines 10 - 12, in this way, documentation over an extended period of time is possible (pg. 6, lines 28 - 29).

By the claimed invention, unauthorized tampering is prevented 9Pg. 4, lines 16 - 18).

Claim 14. A method for monitoring a field device via a data bus with a control unit (Fig. 2 and pg. 4, lines 24,25), comprising the steps of:

using the control unit to request at intervals in time, an individual

identifier of the field device (pg. 4, lines 25,26)'

comparing the requested individual identifier of the field device with an identifier stored in the control unit (pg, 4, lines 26,27), for preventing unauthorized tampering with the field device based on the unauthorized replacement or change of hardware, or software, or even just parts thereof in the field device (pg. 4, lines 27,28); and

producing an alarm or a warning, in the case of a change in the requested individual identifier (pg. 5, lines17- 19

Claim 26. A method for monitoring a field device connected via a data bus with a control unit (Fig. 2 and pg. 4, lines 24,25), comprising the steps of:

directing a query by the control unit to the field device in intervals of time, the query requires an answer from the field dev ice (pg. 6, lines 16 - 18); and

In case no answer comes from the field device, such fact is stored in a data base along with a corresponding time stamp (pg. 5, lines 10-12)

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

(37 CFR 41.37(c)(1)(vi))

In the Office Action of January 13, 2009 the following rejections appear:

1) Claims 14, 15, 21 and 25 are finally rejected under 35 USC 103(a) over Wischinski in view of Ten Brink and Cuzzo et al;

2) Claim 16 is finally rejected under 35 USC 103(a) over Wischinski in view of Ten Brink, Cuzzo et al and Jurisch et al;

3) Claim 17 is finally rejected under 35 USC 103(a) over Wischinski in

view of Ten Brink, Cuzzo et al, Jurisch et al and Aisenberg et al;

4) Claims 18 and 22 - 24 have been finally rejected under 35 USC 103(a) over Wischinski in view of Ten Brink, Cuzzo et al and Havekost et al;

5) Claim 19 is finally rejected under 35 USC 103(a) over Wischinski in view of Ten Brink, Cuzzo et al, Havekost et al and AAPA (Applicant's Admitted prior Art);

6) Claim 26 is finally rejected under 35 USC 103(a) over Wischinski in view of Havekost et al;

7) Claim 27 is finally rejected under 35 USC 103(a) over Wischinski in view of ten Brink, Cuzzo et al, Havekost et al and Alexander, III et al; and

8) Claim 28 is finally rejected under 35 USC 103(a) over Wischinski in view of Ten Brink, Cuzzo et al and Alexander, III et al.

ARGUMENTS

(37 CFR 41.37(c)(1)(vii))

(1)

In rejecting independent claim 14, the examiner combines the teaching of Wischinski, Ten Brink and Cuzzo et al.

First, it is critical that these references teach tamper prevention ***in field devices***. It is respectfully submitted that they do not. For example, Wischinski discloses a system for interrogating an ICS (Industrial Control System) for remote

automation or control devices. On page 2, paragraph 2 of Wischinski there is described a system which includes a device identifier for determining components (hardware, software, firmware) of predetermined automation or control devices indicated in a device data base by periodically querying the devices to have each device indicate its components hardware, software and firmware. By comparison of the available device components with thee components stored in the data base it becomes possible to provide an offer to upgrade installed device components. This is done by a device configuration manager. What does this have to do with the steps recited in claim 14? It is respectfully submitted that the answer is none.

The known system disclosed in Wischinski serves for interrogating an ICS from a remote location to learn what equipment is being used, and in case of an alternative to a piece of equipment being available, to suggest to the owner/operator of the ICS that the piece of equipment be replaced. There is no hint in Wischinski ***that the known system serves for recognizing a tampering of the device***.

The examiner asserts that the feature "using the control unit to request at intervals in time, an individual identifier of the field device," would be known when considering Wischinski. Applicant/Appellant cannot agree. This feature is not disclosed in this way in Wischinski. The examiner is making significant leap in so concluding. One that is not justifying by the disclosure in Wischinski. Wischinski states on page 2, lines 9 - 15 the following: "....and a device configuration manager , responsive to the component identifications in the device database, and further responsive to available device components in a database of available device components, for comparing the installed device components with the available device components and for providing an offer to upgrade installed device components." The abstract states the following: "A system for providing technical support for remote automation or control devices. It includes a device identifier, for determining components of predetermined automation or control devices , such as for example programmable logic controllers ***(not field devices)***, indicated in a data base by periodically querying the devices to have each device indicate its components hardware, software and firmware, the device identifier for providing the

device database with component identification for the predetermined devices; and a device configuration manager, responsive to the components identification in the device database, and further responsive to available device components in a database of available device components, for comparing the installed device components with the available device components and for providing an offer to upgrade installed device components." The periodic querying in Wischinski clearly***has nothing to do with investigating in view of tampering.*** Moreover, Wischinski provides not even a hint that would lead on skilled in the art in the direction of the invention.

In view of the deficiencies in Wischinski, it is respectfully submitted that to combine it with any of the remaining references is really meaningless since it lacks any part of the essence of the present invention as defined in claim 14

Ten Brink goes in a different direction. Ten Brink's solution is based on the concept of permitting only specific devices for operating in automation systems, in particular automatic systems/devices of the SIMATIC series. On page 21 it is stated: "if a device connected to the central processing does not transmit the identification text ' I am an original Siemens device', the central processing denies operation with such a device." Therefore, periodically querying makes no sense in view of Ten Brink.

Wischinski and Ten Brink disclose different embodiments which lack any compatibility, and are therefore not combinable.

Cuzzo et al describes a transmitter and a water system or distribution protection device, such as a fire hydrant protection device. The fire hydrant inhibits an unauthorized individual from accessing water from a water system device. The transmitter, which may be a telemetry transmitter transmits a first signal when the water system protection device is tampered with. One or more sensing devices are provided that sense when the water system protection device has been tampered with, and causes the transmitter to transmit the first signal. Cuzzo et al does not

relate to process automation where field devices and a control unit are connected via a data bus. To add the teaching of Cuzzo et al lacks any real compelling reason when one considers that it relates to water system and the others, including the present invention, do not.

In ***KSR Int'l Co. v. telefax, Inc.*** 550 U.S. 398 (Sp. Ct. 2007) the Supreme Court instructed us to use ***common sense*** in applying 35 USC 103 and in particular the references which are suppose to teach the claimed invention. The Court did not define "common sense" but one can assume that the Court was not employing a new definition. According to the dictionary (Webster's Third New International Dictionary, 1986) one meaning is: "good judgement or prudence in estimating or managing affairs, esp. as free from emotional bias or intellectual subtlety or as not dependent on special or technical knowledge." So one of ordinary skill in the art, even discounting any technical knowledge, would have to conclude that the proposed combination of Wischinski, Ten Brink and Cuzzo et al cannot be combined because none but Cuzzo et al are at all concerned with tamper prevention, and Cuzzo et al does not relate to field devices, which the present invention is.

(2)

Independent claim 26, we do not see any teaching in Wischinski or Havekost et al, that relates to time stamp feature recited therein.

The examiner refers us to "(Abstract (block 66), figures 5 - 7 (see days with times) col. 10, lines 23 - 29, col. 10 lines 23 - 29, col. 14 line 67, col. 15 lines 1 - 4, 18 - 21, 38 - 41) and suggests that these passages teach "in case no answer comes from the field device, such fact is stored in a database along with a corresponding time stamp." But this quoted conclusion cannot be found in the referenced passages of Havekost et al. Even so, Wischinski is defective for the reasons noted above, and it is respectfully submitted that Havekost et al cannot salvage the noted defects.

As to the remaining references of record, it is respectfully submitted that they too do not provide sufficient teaching to somehow cancel the defects in Wischinski.

CONCLUSION

In view of the fact that the references applied by the examiner against the pending claims lack one or more of the steps claimed to avoid tampering, it is respectfully submitted that claims 14 - 19 and 21 - 28 should be allowed over the references of record.

Respectfully submitted
BACON & THOMAS, PLLC

Date: March 8, 2010

Felix J. D'Ambrosio
Reg. No. 25,721

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, VA 22314
Tel: (703) 683-0500
Fax: (703) 683-1080

S:\Producer\fjd\CLIENTS\Endress+Hauser Holding GmbH\DEGR3003-PS0019\Brief on Appeal Corrected Nov. 19, 2009.wpd

APPENDIX OF CLAIMS
(37 CFR 41.37 (c)(1)(viii)

14. A method for monitoring a field device connected via a data bus with a control unit, comprising the steps of:

using the control unit to request at intervals in time, an individual identifier of the field device;

comparing the requested individual identifier of the field device with an identifier stored in the control unit, for preventing unauthorized tampering with the field device based on the unauthorized replacement or change of hardware, or software, or even just parts thereof in the field device; and

producing an alarm or a warning, in the case of a change in the requested individual identifier.

15. The method as claimed in claim 14, wherein:

the individual identifier is the serial number of the field device.

16. The method as claimed in claim 14, wherein:

the individual identifier is a key in the device firmware of the field device.

17. The method as claimed in claim 16, wherein:

the individual identifier is a test sum of a memory unit in the field device.

18. The method as claimed in claim 14, further comprising the step of:

storing the requested individual identifier in a database, along with a time stamp.

19. The method as claimed in claim 18, wherein:

a storing in the database only occurs, when a change is detected in the requested individual identifier.

21. The method as claimed in claim 14, wherein:

the alarm or warning is only produced, when the change occurs outside of a specified time period for maintenance.

22. The method as claimed in claim 14, wherein:
the alarm or warning is presented at the control unit.

23. The method as claimed in claim 14, wherein:
the alarm or warning is sent in electronic form.

24. The method as claimed in claim 14, wherein:
the alarms or warnings are retrievable at the control unit.

25. The method as claimed in claim 14, wherein:
the alarms or warnings can be retrieved via a client.

26. A method for monitoring a field device connected via a data bus with a control unit, comprising the steps of:

directing a query by the control unit to the field device in intervals of time, the query requires an answer from the field device; and

in case no answer comes from the field device, such fact is stored in a data base along with a corresponding time stamp.

27. The method as claimed in claim 23, wherein:
the electronic form is one of: email; SMS; and fax.

28. The method as claimed in claim 25, wherein:
the alarms or warnings can be retrieved via Internet Explorer.

EVIDENCE APPENDIX

There is no evidence being relied upon which was submitted pursuant to 37 CFR 1.130, 1.131 or 1.132.

RELATED PROCEEDINGS APPENDIX

There is no related proceeding being relied upon.